Rohan Desai

> Cybersecurity Analyst (Threat Intelligence)
>
> 📧 rohan.desai.sec@email.com | 📞 +91 98765 43212 | 📍 Pune, Maharashtra

Summary

A proactive Cybersecurity Analyst with over 7 years of experience in threat intelligence, incident response, and security operations. Specializes in analyzing threat actor TTPs, reverse-engineering malware, and creating actionable intelligence to fortify security postures. Proficient with SIEM platforms, EDR solutions, and threat intelligence platforms (TIPs).

Technical Skills

- **SIEM & Log Analysis:** Splunk, ELK Stack, QRadar
- **Endpoint Security:** CrowdStrike Falcon, Carbon Black, Windows Defender ATP
- **Threat Intelligence:** MISP, ThreatConnect, Recorded Future
- **Malware Analysis:** Ghidra, IDA Pro, Wireshark, Volatility
- **Scripting:** Python, PowerShell
- **Frameworks:** MITRE ATT&CK, NIST Cybersecurity Framework

Professional Experience

Senior Threat Intelligence Analyst | SecureNet Corp. | Pune, India *(Jun 2020 - Present)*

- Leads the threat intelligence program, providing timely and actionable reports on emerging threats to stakeholders.
- Conducted deep-dive analysis on ransomware families, identifying key indicators of compromise (IOCs) that were used to create detection rules in Splunk.
- Automated the ingestion of threat feeds into MISP using Python, saving 10 hours of manual work per week.
- Served as a key member of the incident response team during critical security events, performing forensic analysis and containment.

Cybersecurity Analyst | Global Bank | Mumbai, India *(May 2017 - May 2020)*

- Monitored security alerts in a 24/7 Security Operations Center (SOC).
- Investigated and triaged security incidents, escalating as necessary.
- Developed custom dashboards in Splunk to visualize security metrics.

Projects

Phishing Campaign Analysis

- Analyzed a large-scale phishing campaign, reverse-engineered the malware payload, and provided a detailed report on the attacker's infrastructure and methods.

Education

Bachelor of Science in Information Technology *University of Mumbai* | Mumbai, India *(2013 - 2017)*

- **Certifications:** CompTIA Security+, GIAC Certified Intrusion Analyst (GCIA)